UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES, Plaintiff, v. DUMAKA HAMMOND, Defendant.	Case No. 16-cr-00102-JD-1 **ORDER RE MOTIONS TO SUPPRESS AND DISMISS** Re: Dkt. Nos. 19, 30, 31, 32

This case raises the question of whether evidence obtained under a search warrant issued in excess of a magistrate judge's authority should be suppressed. Under controlling Ninth Circuit authority, the answer is no. This case also raises the question of whether the defendant should have been advised of his *Miranda* rights before making incriminating statements to law enforcement officers during an interrogation at dawn in his home. This evidence must be suppressed.

BACKGROUND

The background facts are largely undisputed. Defendant Dumaka Hammond is a registered sex offender with two prior convictions for possession of child pornography. In July 2015, an FBI special agent applied to a magistrate judge in this district for a search warrant for Hammond's home in Richmond, California. The application stated that an IP address linked to an online child pornography site had been traced to a Comcast account in Hammond's name and with his home address.

The FBI linked Hammond to the online site during an investigation under a search warrant issued in the Eastern District of Virginia. In January 2015, the FBI had seized in North Carolina a server hosting a website known as "Playpen." Playpen was a website dedicated to child pornography, including discussion forums and a multitude of images and videos organized by

various categories. Users could access the Playpen website only through the Tor network, a free online network designed to anonymize a user's actual IP address and hide his true location by routing Internet activities through thousands of volunteer relay computers. Playpen required a username, password and e-mail account for access but it expressly warned users not to enter their real e-mail addresses.

After seizing Playpen, the government decided to keep it in operation on a government server housed in Newington, Virginia in order to locate and identify Playpen users. To that end, the government filed in the Eastern District of Virginia an application for a search warrant authorizing the use of a Network Investigative Technique ("NIT") to work around the anonymizing technology of Tor and uncover the identity of Playpen users. The NIT was software that would be deployed on the Playpen website and sent to the computer of any user or administrator who logged into Playpen with a username and password. Once embedded in the user's computer, the NIT would cause the computer to send back to the FBI its IP address and other identifying information. The warrant application sought authorization to deploy the NIT to any user who accessed Playpen wherever the user was located, regardless of whether the user's geographic location was inside or outside the Eastern District of Virginia.

On February 20, 2015, a magistrate judge in the Eastern District of Virginia signed the warrant authorizing use of the NIT for a 30-day period. On the same day, the government also obtained authorization of a separate wiretap order -- to intercept the communications taking place on Playpen -- from a district judge in the Eastern District of Virginia. On March 4, 2015, the government decided to terminate the NIT search and take Playpen permanently offline, after approximately two weeks of operation. Hammond accessed Playpen while the warrant was in effect and the NIT sent his user information to the FBI, which resulted in the search warrant issued in this district.

The search warrant here was issued by a magistrate judge on July 16, 2015, and executed the next morning. Twelve federal special agents from the FBI and the U.S. Postal Inspectors, and three federal and state non-officers (a state senior investigator and two FBI support personnel) arrived at Hammond's home at approximately 6 a.m. There were also two marked Richmond

police department cars that were present during at least the initial service of the warrant. Hammond was only half-dressed and was not wearing a shirt when the law enforcement personnel arrived. He saw at least one officer holding a gun. Hammond and his mother, sister and fourteen-year-old niece were all initially handcuffed outside the house while the officers searched the interior of Hammond's home. Hammond was later interviewed in his bedroom. His handcuffs were removed for the interview, but he remained shirtless. There were at least two agents in the room with Hammond, and the door to his bedroom was closed. Hammond was interviewed for 65 minutes, and he was not at any point read his rights under *Miranda v. Arizona*, 384 U.S. 436 (1966). At the conclusion of his interview, he signed a written statement in which he confessed to and apologized for viewing child pornography.

DISCUSSION

I. SUPPRESSION OF THE NIT WARRANT (DKT. NOS. 19, 31)

Hammond challenges only the NIT warrant issued by the magistrate judge in the Eastern District of Virginia, and not the search warrant for his home that was issued by the magistrate judge in this district. He challenges the NIT warrant on two separate grounds: that it violated Federal Rule of Criminal Procedure 41 and the Fourth Amendment's particularity requirement. Dkt. Nos. 19, 31.

The first question is whether a warrant was needed at all for the NIT to be deployed. The government takes the position that it was not because Hammond had no reasonable expectation of privacy in his IP address. That argument might have carried the day if the government had obtained Hammond's IP address from a third party, *see U.S. v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2008), but here, the government obtained it directly from Hammond's computer via the NIT. This distinction makes all the difference. *See, e.g.*, *Riley v. California*, 134 S.Ct. 2473, 2492-93 (2014) (distinguishing between using a pen register at a telephone company's premises, which is "not a 'search' at all," versus the police searching a defendant's cell phone directly, even if for the call log only).

In *Riley*, the Supreme Court took a significant step in advancing Fourth Amendment standards into the digital age. Among other holdings, the Court underscored the fact that modern

cell phones are effectively "minicomputers" with immense storage capacity that users rely on for "a digital record of nearly every aspect of their lives -- from the mundane to the intimate." *Id*. at 2490. Consequently, a law enforcement search of a cell phone directly implicates the user's privacy interests. *Id*. at 2489-90. These privacy concerns apply equally and arguably even more strongly to law enforcement's search of a laptop computer. *Cf. U.S. v. Bare*, 806 F.3d 1011, 1021 (9th Cir. 2015) (Kozinski, J., dissenting) (search of a defendant's laptop computer would "certainly do no less" than the search of a cell phone in "allowing police to reconstruct '[t]he sum of an individual's private life.'") (quoting *Riley*, 134 S.Ct. at 2489); *U.S. v. Kim*, 103 F. Supp. 3d 32, 54 n.14 (D.D.C. 2015) ("The fact that *Riley* involved a cellular telephone rather than a laptop is of little moment; indeed, it was the fact that a cellular telephone is, for all intents and purposes, a small computer, that led that Court to find that the usual rules governing a search incident to arrest should not apply."); *U.S. v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015) (finding that "under *Riley*, the nature of the electronic device greatly increases the potential privacy interests at stake," and noting that a laptop computer is a "device with even greater [storage] capacity than the cell phones at issue in *Riley*").

Riley also found that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." 134 S.Ct. at 2491 (emphasis in original). Another district court faced with a NIT warrant challenge persuasively applied this same house analogy to the facts here: "[i]f a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper -- even accepting that the defendant had no reasonable expectation of privacy in the IP address itself." *U.S. v. Croghan*, No. 1:15-cr-48, 2016 WL 4992105, at *7 (S.D. Iowa Sept. 19, 2016). So too here. Even if Hammond may not have had an expectation of privacy in the ultimate object of the NIT warrant -- his IP address -- a warrant was needed before the FBI could search his laptop computer for that information through the Network Investigative Technique.

The next question is whether the warrant that was obtained was proper.[1] Hammond challenges the warrant under the Fourth Amendment's particularity requirement. *See* Dkt. No. 31. Like the majority of courts looking at the issue, the Court finds that the NIT warrant was sufficiently particularized. *See, e.g., U.S. v. Henderson*, Case No. 15-cr-565-WHO, 2016 WL 4549108, at *4 (N.D. Cal. Sep. 1, 2016) (citing cases).

Hammond likens the NIT warrant to the overbroad warrant that was invalidated in *U.S. v. Bridges*, 344 F.3d 1010 (9th Cir. 2003). But there is a night-and-day difference between them. In *Bridges*, the list of items that were to be seized contained at least thirteen different categories with multiple subparts, and the list was "so expansive that its language authorize[d] the Government to seize almost all of ATC's property, papers, and office equipment in Billings." *Id*. at 1017. This problem was compounded by the fact that the warrant at issue did "not state what criminal activity is being investigated by the IRS." *Id*. at 1018. None of that applies here. The NIT warrant clearly states that the NIT is to be deployed on "the server operating the Tor network child pornography website" as identified by its Tor URL. Dkt. No. 19-2, Ex. A. The NIT is to gather information only from "activating computers," which are "those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." *Id*., Attachment A. The information to be gathered is clearly listed as seven specific items, including the activating computer's "actual IP address," "the type of operating system running on the computer," the activating computer's "operating system username," and its "media access control ('MAC') address." *Id*, Attachment B. This is a sufficiently particularized warrant under the Fourth Amendment, and the mere fact that the government could have drawn up a narrower warrant if it wished to do so does not change that conclusion.

//

//

//

[1] Because a warrant was obtained here and suppression is not granted, the Court need not consider the government's back-up argument that the search was proper under "exigent circumstances." Dkt. No. 27 at 19-20.

Federal Rule of Criminal Procedure 41 is, however, a different matter, and the Court finds that the warrant did not comply with that rule.[2] The NIT warrant was issued by a federal magistrate judge, and Rule 41 places geographic limits on the scope of a magistrate judge's authority to issue a warrant. *See, e.g.*, Fed. R. Crim. P. 41(b)(1) ("At the request of a federal law enforcement officer or an attorney for the government a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district"). The critical issue here is that the magistrate judge in the Eastern District of Virginia signed off on a warrant that authorized the search of "activating computers" located outside of her district. Tellingly, the affidavit in support of the warrant specifically requested authority to embed the NIT on any "activating computer -- *wherever located*." Dkt. No. 19-2, Ex. A, Affidavit ¶ 46(a) (emphasis added).

The government tries to shoehorn this exercise of authority into Rule 41 subsections (b)(1) (authority to issue warrant for search and seizure of "person or property *located within the district*"), (2) (authority to issue warrant for "person or property outside the district if the person or property is *located within the district when the warrant is issued* but might move or be moved outside the district before the warrant is executed") and (4) (authority to issue warrant "*to install within the district* a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both"). But as the italicized language makes clear, in order for these subsections to apply, the Court would need to accept a version of the facts that is more Tomorrowland than truth. The government says that the NIT was installed on activating computers in the Eastern District of Virginia because Playpen users "made a virtual trip via the Internet to the Eastern District of Virginia," and Hammond's computer "entered the Eastern District of Virginia by accessing the Playpen website, which resided on a server in that District [and] retrieved the NIT from that server." Dkt. No. 27 at 16-17.

[2] Hammond has also referenced the Federal Magistrates Act, 28 U.S.C. § 636(a), but he makes clear in his papers that he is not invoking that statute as a separate ground for suppression. His reference to the act was only to note that "§ 636(a) cannot expand a magistrate judge's authority beyond the limits of Federal Rule of Criminal Procedure 41." Dkt. No. 42 at 4 n.4. As such, the Court does not separately analyze the NIT warrant under 28 U.S.C. § 636(a).

That, of course, is not at all how the NIT worked in the real world. As the affidavit for the NIT warrant explained, it worked by placing "additional computer instructions" in the content the Playpen website would normally send to users. Dkt. No.19-2, Ex. A, Affidavit ¶ 33. "When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." *Id*. While the instructions may have resided on the Playpen server in the Eastern District of Virginia, Hammond became subject to the NIT only at the point when those instructions were downloaded to his computer. Hammond's computer is a physical object that at all times remained in his home in the Northern District of California, and the download, too, occurred here and not "virtually" in the Eastern District of Virginia. Authorizing this kind of out-of-district search was beyond the Eastern District of Virginia magistrate judge's authority under Federal Rule of Criminal Procedure 41. *See also*, *e.g.*, *Henderson*, 2016 WL 4549108, at *3-4 (and cases therein).[3]

So the magistrate judge's authorization of the NIT warrant violated Rule 41. The Court has already rejected defendant's only constitutional objection to the warrant (based on the Fourth Amendment's particularity requirement), and consequently this error is a "technical" error rather than a "fundamental" one. *U.S. v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992) (dividing Rule 41 violations into two categories, fundamental and technical, and explaining that "[f]undamental errors are those that result in clear constitutional violations"). The next issue is what to do about this technical error. "[S]uppression is rarely the proper remedy for a Rule 41 violation." *U.S. v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006). And the underlying purpose of the exclusionary rule is to "deter police misconduct, not that of judges and magistrates." *Negrete*, 966 F.2d at 1283. Therefore, technical errors like the one here "require suppression only if: (1) the defendants were prejudiced by the error, or (2) there is evidence of deliberate disregard

[3] The Court does not in any event find the NIT to have been a "tracking device" under Rule 41(b)(4). *See*, *e.g.*, *Henderson*, 2016 WL 4549108, at *3-4; *U.S. v. Levin*, Case No. 15-10271-WGY, 2016 WL 2596010, at *6 (D. Mass. May 5, 2016).

of the rule. Prejudice in this context means the search would otherwise not have occurred or would have been less intrusive absent the error." *Negrete*, 966 F.2d at 1283.

Two cases from our circuit court illustrate what prejudice means in this context and show why it is absent here. In *U.S. v. Ritter*, 752 F.2d 435, 440 (9th Cir. 1985), there was no dispute that "Rule 41 was violated when a search of Ritter's residence was conducted pursuant to a telephonic search warrant authorized by a state, rather than a federal, magistrate." Nevertheless, the court affirmed the trial court's finding that defendant was not prejudiced by this technical violation because there was "no indication that a federal magistrate would have handled the search warrant application differently than did the state judge." *Id*. at 441. Similarly, in *U.S. v. Luk*, 859 F.2d 667, 673 (9th Cir. 1988), the court found a technical violation of 41(a) because the record did not show "either that the actual request for the warrant came from Assistant United States Attorney Rossbacher or that Rossbacher asked the magistrate to issue the warrant to Agent Koplik." Again, however, the court found no prejudice to defendant where there was "no reason to believe that the federal magistrate who reviewed the affidavit and warrant application presented by Agent Koplik would have proceeded differently or not authorized the search warrant if Rossbacher had himself called directly to 'request' the warrant or requested it in person." *Id*. at 674.

As these cases establish, the prejudice inquiry asks whether the warrant would not have been issued had the rules been followed properly. If the answer is that the warrant would still have been issued and the search still would have occurred in a manner that was compliant with the rules, there is no prejudice to defendant and no suppression is required. That is the case here. Hammond himself pointed to this conclusion when he forthrightly acknowledged that "a district judge -- as opposed to a magistrate judge -- could issue a warrant regardless of the jurisdictional limitations of Rule 41." Dkt. No. 42 at 3 (citing *U.S. v. Levin*, Case No. 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016)).[4] Rule 41 expressly speaks to the authority of federal magistrate judges to issue warrants. United States district judges derive their authority from

[4] He later tried to run from it when the implications became clearer to him, Dkt. No. 52, but his first impression was right.

Article III of the Constitution, and they are deemed to have inherent power to issue a warrant when the requirements of the Fourth Amendment are met, whether the warrant directs the search of property located inside or outside the judicial district in which the district judge happens to sit. *See Levin*, 2016 WL 2596010, at *14 ("With respect to district judges, neither Rule 41(b) nor Section 636(a) of the Federal Magistrates Act restricts their inherent authority to issue warrants consistent with the Fourth Amendment."). So here, the government could have properly sought issuance of the NIT warrant by a district judge in the Eastern District of Virginia, and there is no reason at all to think that such a request would have been denied. To the contrary, Hammond himself has argued that "[t]he government obtained authorization by a district judge to intercept communications and could have asked that district judge to authorize the deployment of the NIT as well." Dkt. No. 42 at 3. Under *Ritter* and *Luk*, Hammond has failed to establish the necessary prejudice that would require suppression for the technical Rule 41 violation that occurred here.

Hammond has also failed to show that the government manifested a "deliberate disregard" of Rule 41, which might have independently supported suppression. *Negrete*, 966 F.2d at 1283. Hammond presents as his "most pertinent" piece of evidence on this point a 2013 decision by a magistrate judge in the Southern District of Texas rejecting the government's request for a search warrant that was "remarkably similar to the NIT warrant." Dkt. No. 19 at 16 (citing *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013)). This single decision is insufficient to show that "the government" as a whole was "on notice" that warrants like the NIT warrant were improper. *Id*. Moreover, Hammond has made no effort whatsoever to show that any specific person in the Eastern District of Virginia who was actually associated with the procurement of the NIT warrant had any knowledge or intent that would support a finding of deliberate disregard of Rule 41. That an amendment to Rule 41 (clarifying the propriety of warrants like the NIT warrant, *i.e.*, warrants authorized by magistrate judges to remotely search computers whose locations are not known) was pending when the NIT warrant was issued also falls far below the bar of evidence that establishes deliberate disregard. The amendment effort shows nothing more than an intention on the part of the Judicial Conference's Committee on Rules of Practice and Procedure to keep the rules more current with the times. The

Court finds that there is no evidence of "deliberate disregard" here that would support the extreme remedy of suppression.

Defendant's motions to suppress the NIT warrant and all of its evidentiary "fruits" are consequently denied.

II. DISMISSAL FOR OUTRAGEOUS GOVERNMENT CONDUCT (DKT. NO. 32)

Focusing on a different aspect of the government's deployment of the NIT, Hammond seeks dismissal of his indictment in its entirety. He asserts that the "government's operation of a child pornography website from February 20, 2015 until March 4, 2015 that caused thousands of child pornography links, images, and videos to be posted, viewed, and distributed" constitutes outrageous government conduct supporting dismissal of the indictment. Dkt. No. 32.

To be sure, the government's decision to run a child pornography website on its own servers raises troubling questions. The digital nature of the images and videos that were hosted means there is no way to stop them from continuing to be shared, and the government itself has rightly taken the position that "young victims are harmed every time an image is generated, every time it is distributed, and every time it is viewed." Dkt. No. 32 at 8-9 (quoting government press release). The government itself clearly had qualms about the operation, as it took it down on its volition after only two weeks, even though it had authorization to deploy the NIT for a full 30 days.

But the facts here do not meet the "extremely high standard" for dismissing an indictment for outrageous government conduct. *U.S. v. Black*, 733 F.3d 294, 302 (9th Cir. 2013). Dismissal under that doctrine is warranted only in those "extreme cases in which the defendant can demonstrate that the government's conduct violates fundamental fairness and is so grossly shocking and so outrageous as to violate the universal sense of justice." *Id*. at 302 (internal quotations omitted). Having considered the six relevant factors that are set out in *Black* -- which are intended not to "constitute a formalistic checklist, but [to] help focus [the Court's] analysis of the totality of circumstances," *id*. at 304 -- the Court joins the other courts that have denied similar motions. *See, e.g., U.S. v. Allain*, Case No. 15-cr-10251, 2016 WL 5660452, at *12-13 (D. Mass. Sept. 29, 2016); *U.S. v. Anzalone*, Case No. 15-10347-PBS, 2016 WL 6476939, at *1 (D. Mass.

Oct. 28, 2016); *U.S. v. Owens*, Case No. 16-CR-38-JPS, 2016 WL 7079617, at *1 (E.D.Wis. Dec. 5, 2016). While unsavory, the government's conduct did not rise to the level of outrageousness needed to support the dismissal of defendant's indictment.

III. SUPPRESSION OF THE INTERROGATION EVIDENCE (DKT. NO. 30)

Hammond has also moved for an order suppressing the statements he gave to the FBI on July 17, 2015, on the basis that the interrogation violated his constitutional rights under *Miranda v. Arizona*, 384 U.S. 436 (1966). Dkt. No. 30.

The controlling case for this issue is *U.S. v. Craighead*, 539 F.3d 1073 (9th Cir. 2008). Judge Bybee squarely and eloquently addressed police interrogations conducted within the home, emphasizing the uniqueness of that setting as described by the poet Robert Frost: "Home . . . is the place where, when you go there, they have to take you in." *Id*. at 1082-83. As in that case, the parties here agree that Hammond was "interrogated but not given *Miranda* warnings. Therefore, the only issue . . . is whether [Hammond] was in custody at the time of his interrogation." *Id*. at 1082.

Craighead directs that, to distinguish a custodial in-home interrogation from a non-custodial one, the key question the Court is to consider is "the extent to which the circumstances of the interrogation turned the otherwise comfortable and familiar surroundings of the home into a 'police-dominated atmosphere.'" 539 F.3d at 1083. This determination is "necessarily fact intensive," and several factors are relevant: "(1) the number of law enforcement personnel and whether they were armed; (2) whether the suspect was at any point restrained, either by physical force or by threats; (3) whether the suspect was isolated from others; and (4) whether the suspect was informed that he was free to leave or terminate the interview, and the context in which any such statements were made." *Id*. at 1084.

These factors point to a custodial in-home interrogation in this case. First, there were fourteen law enforcement officers (twelve from the FBI and U.S. Postal Inspectors, and assuming at least one officer in each of the two marked Richmond police department cars) who arrived at Hammond's home at 6 a.m. the morning of the search. This is considerably more than the eight who were present at the defendant's home in *Craighead*. It is not disputed that Hammond saw at

least one officer holding a gun. Dkt. No. 30-2, Ex. B ¶ 4. Second, Hammond was placed in handcuffs prior to his interview, though they were removed during the interview itself. The *Craighead* court took note of another decision in which handcuffing of a suspect upon entry into her home by law enforcement was found to have "contributed to a custodial environment." 539 F.3d at 1085 (citing *U.S. v. Revels*, 510 F.3d 1269, 1276-77 (10th Cir. 2007)). Third, Hammond was isolated from his mother, sister and niece. Only he was brought into his bedroom. Dkt. No. 30-2, Ex. B ¶¶ 8-9.

On the fourth factor, it is true that Hammond was repeatedly told that he was not going to be arrested that day. *See, e.g.*, Dkt. No. 30-2, Ex. C at 2:15-23, 32:11-12. "The mere recitation of the statement that the suspect is free to leave or terminate the interview, however, does not render an interrogation non-custodial *per se*." *Craighead*, 539 F.3d at 1088. Here, no less than fourteen law enforcement officers had swarmed Hammond's home at the crack of dawn, with at least one officer holding a gun. Hammond was interviewed while being only half-dressed, with multiple armed agents in his bedroom with the door closed. Hammond and his family members were in handcuffs just moments before the start of the in-home interrogation. Hammond has declared under penalty of perjury that he "did not feel free to leave." Dkt. No. 30-2, Ex. B ¶ 13. In these circumstances, the Court concludes that even if Hammond may have been told that he was free to leave and that his statements were voluntary, "a reasonable person in [Hammond's] position would not have actually 'felt' he was free to leave." *Craighead*, 539 F.3d at 1089 (citation omitted).

Considering the totality of the circumstances, the Court concludes that the interrogation of Hammond in his home was custodial, and *Miranda* warnings were consequently required. Because they were not given, Hammond's oral and written statements to the FBI agents on July 17, 2015, must be suppressed.

CONCLUSION

The Court denies defendant's motions to suppress the NIT warrant and its evidentiary fruits. Defendant's motion to dismiss the indictment for outrageous government conduct is also

denied. The Court grants defendant's motion to suppress the statements he gave to the FBI on July 17, 2015.

This order terminates docket numbers 19, 30, 31 and 32.

IT IS SO ORDERED.

Dated: December 8, 2016

JAMES DONATO
United States District Judge

United States District Court
Northern District of California